

# Identifying Codes of Degree 4 Cayley Graphs over Abelian Groups

Cristóbal Camarero and Carmen Martínez and Ramón Beivide

## Abstract

In this paper a wide family of identifying codes over regular Cayley graphs of degree four which are built over finite Abelian groups is presented. Some of the codes in this construction are also perfect. The graphs considered include some well-known graphs such as tori, twisted tori and Kronecker products of two cycles. Therefore, the codes can be used for identification in these graphs. Finally, an example of how these codes can be applied for adaptive identification over these graphs is presented.

## 1 Introduction

Systems are continuously growing in complexity, thus becoming composed of more and more basic elements. This originates many important problems which must be solved in order to use the systems effectively. Among these problems are the parallelization of algorithms to exploit the full system, the development of networks efficient in cost and in performance, and the automatic detection of failures, and consequently, reconfiguration and recovery of the system.

In this paper the problem of the detection of faults will be explored, with principal aim at multiprocessor systems, in which the basic elements are computers. These computers are connected between them with some topology which can be modeled by a (usually undirected) graph. The graphs under consideration will be regular Cayley graphs of degree four, which englobe a multitude of well-known interconnection networks.

The major mechanisms for fault-diagnosis are the PMC model by Preparata, Metzger and Chien [17] and the comparison model by Malek [14]. In the PMC model, each unit tests each neighbor to see if it is faulty and the tests performed by faulty units are unreliable. Then, all the information is used globally to determinate the faulty vertices. A bit of information is generated for each edge and direction, which is a considerable volume of information. Later, Karpovsky, Chakrabarty and Levitin in [12] proposed identifying codes with the aim of reducing the necessary information for fault diagnosis.

Identifying codes can be seen as a subset of vertices of a graph which allows the identification of single vertices under some conditions. When identifying codes apply for diagnosis, for each codeword a bit of information is generated, which is significant less information than the number of edges, as required in the PMC model. Since minimizing the global information is equivalent to minimizing the density of the code, a lot of work has been done to find codes with minimum density over different infinite graphs. There are hundreds of papers [13] on identifying codes, many of them looking for the ones which attain the minimal density bound over different graphs. However, there are not many constructive methods for finding wide families of these codes over graphs which correspond to topological models for multiprocessor systems. Moreover, technical aspects of the diagnosis process using identifying codes have not been extensively considered. An algorithmic approach to the adaptive identification in multiprocessor systems has been considered, for example in [2] and [20].

In this paper a constructive method for finding a wide family of identifying codes over degree four Cayley graphs over finite Abelian groups is provided. The codes are built using subgroups, which implies that the codewords are evenly distributed. The identifying radius as well as the covering radius are characterized in terms of the generators of the subgroup. Moreover, such codes in some cases are also perfect codes, but for a different radius than the identifying one. Hence, in Section 2 the graphs that are going to be considered in the paper are defined. In Section 3 some basic definitions of identification are recalled and a few new ones that will be needed to make the general construction are established. In Section 4 the identifying radius for a family of group codes is determined. Moreover, both the case in which the codes constructed are not only identifying but also perfect, and the density of the construction are considered. Finally in Section 5 an example of how to apply these codes for adaptive identification in faulty environments modeled by Cayley graphs is shown. Some of the results presented in this paper were first announced in [5].

## 2 Cayley Graphs over Two Dimensional Lattices

In this section some definitions and results concerning two dimensional lattices are introduced. Then, degree four regular Cayley graphs over these lattices are defined for obtaining a metric space in which identifying and perfect codes are possible to be constructed.

Given two linearly independent integer vectors  $m_1, m_2 \in \mathbb{Z}^2$  let us consider

$$\langle m_1, m_2 \rangle = \{ \lambda_1 m_1 + \lambda_2 m_2 \mid \lambda_i \in \mathbb{Z}, i = 1, 2 \},$$

the integer lattice (or additive group) generated by vectors  $m_1, m_2$ . As usual, the quotient group can be defined as:

$$\mathbb{Z}^2 / \langle m_1, m_2 \rangle \mathbb{Z}^2 = \{ v + \langle m_1, m_2 \rangle \mid v \in \mathbb{Z}^2 \}.$$

The following theorem will be used (for the proof see [8]):

**Theorem 2.1.**  $\mathbb{Z}^2/\langle m_1, m_2 \rangle \mathbb{Z}^2$  has  $|\det(M)|$  elements, where  $M$  is the matrix whose columns are the linearly independent vectors  $\{m_1, m_2\}$ .

Following the notation in [8], two vectors  $v_1, v_2$  in the same coset of the quotient group  $\mathbb{Z}^2/\langle m_1, m_2 \rangle \mathbb{Z}^2$  will be denoted as  $v_1 \equiv v_2 \pmod{M}$ . The quotient group  $\mathbb{Z}^2/\langle m_1, m_2 \rangle \mathbb{Z}^2$  will be denoted as  $\mathbb{Z}^2/M\mathbb{Z}^2$  and a subgroup  $\langle t_1, t_2 \rangle \subseteq \mathbb{Z}^2/\langle m_1, m_2 \rangle \mathbb{Z}^2$  as  $T + \mathbb{Z}^2/M\mathbb{Z}^2$ , where  $T$  is the matrix whose columns are  $t_1$  and  $t_2$ . As usual,  $\mathcal{M}_{2 \times 2}(\mathbb{Z})$  denotes the ring of the square integer matrices of size two. In the remainder of the paper, it will be assumed  $M \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$  to be non-singular.

The Cayley graphs considered in the paper are defined over two-dimensional lattices. As usual, a Cayley graph is defined:

**Definition 2.2.** The *Cayley graph* over a group  $\Gamma$  and a set  $A \subset \Gamma$  is the graph  $\text{Cay}(\Gamma; A)$  with vertex set  $V = \Gamma$  and edges

$$E = \{(v, v + g) \mid v \in \Gamma, g \in A\}$$

The set  $A$  is called the *adjacency set*.

In this paper Cayley graphs over the quotient rings defined above are going to be considered. Therefore, given  $M \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$  a non-singular matrix and  $A = \{a_1, a_2\}$  a subset of vectors of  $\mathbb{Z}^2$ , the Cayley graph over the group  $\mathbb{Z}^2/M\mathbb{Z}^2$  with adjacency  $A \subset \mathbb{Z}^2$  will be denoted by  $\mathcal{G}(M; A)$ . Therefore, every vertex  $u \in \mathbb{Z}^2/M\mathbb{Z}^2$  of  $\mathcal{G}(M; A)$  is adjacent to  $u \pm A \pmod{M}$ . Moreover, for convenience,  $E = \{e_1, e_2\}$  will denote the orthonormal two-dimensional basis, where  $e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  and  $e_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . Without loss of generality, it can be assumed that any  $\mathcal{G}(M; A)$  has as set of jumps  $A = E$ . Therefore,  $\mathcal{G}(M) = \mathcal{G}(M; E)$ . This way, any  $\mathcal{G}(M)$  is locally a two-dimensional orthogonal mesh, with wrap-around edges completing the peripheral adjacency. The graphs considered in the present paper constitute the two dimensional case of the general family of multidimensional circulants defined in [8]. Moreover, as it is stated in the following result, these are in fact all the Cayley graphs of degree four over finite Abelian groups.

**Lemma 2.3.** [4] Let  $\Gamma$  be a finite Abelian group,  $A = \{\pm a, \pm b\} \subseteq \Gamma$  and consider  $\text{Cay}(\Gamma; A)$ . Then, there exists  $M \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$  such that

$$\text{Cay}(\Gamma; A) \cong \mathcal{G}(M).$$

Many topological models for interconnection networks are in fact Cayley graphs as the ones that are being considered in this paper. For example, tori, twisted tori [18] and circulant graphs of degree four such as the ones in [19] and [9]. As it was proved in [16], also the Kronecker product of two cycles is a particular case of  $\mathcal{G}(M)$ .

**Example 2.4.** Let  $M = \begin{pmatrix} 12 & 5 \\ 1 & 5 \end{pmatrix}$ . In Figure 1 a graphical representation of the graph  $\mathcal{G}(M)$  in which the representative at minimum distance from zero of every vertex is shown.

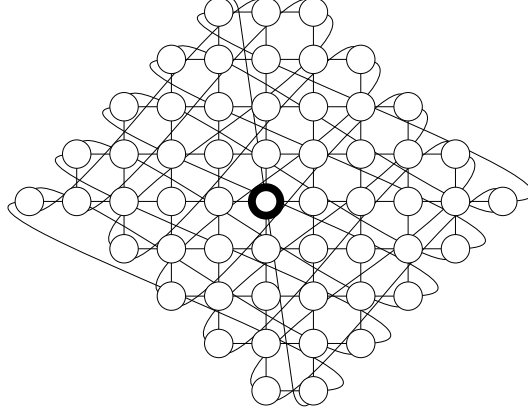


Figure 1:  $\mathcal{G}(M)$  represented in minimum distances.

Finally, if  $d_M(v_1, v_2)$  denotes the distance between vertices  $v_1$  and  $v_2$  of  $\mathcal{G}(M)$ , then it can be calculated as:

$$d_M(v_1, v_2) = |\lambda_1| + |\lambda_2|,$$

with  $\lambda_1, \lambda_2 \in \mathbb{Z}$  such that

$$v_1 - v_2 \equiv \lambda_1 e_1 + \lambda_2 e_2 \pmod{M}$$

and  $|\lambda_1| + |\lambda_2| \neq 0$  being minimum.

### 3 Previous Definitions on Identification

The *ball* of radius  $r$  centered at  $v \in V$  is defined as:

$$B_r(v) = \{w \in V \mid d(v, w) \leq r\}.$$

Then, it is also said that a vertex  $v$  *r-covers*  $w$ , for any  $w \in B_r(v)$ . A *code*  $\mathcal{C}$  is a nonempty set of vertices, whose elements are called *codewords*. Given a vertex  $v \in V$  the set of codewords which *r-cover*  $v$  are denoted as:

$$K_r(v) = \mathcal{C} \cap B_r(v).$$

Moreover, two vertices  $v, w \in V$  are said to be *r-separated* if  $K_r(v) \neq K_r(w)$ .

**Definition 3.1.** [12] A code  $\mathcal{C}$  of a graph  $G$  is said *r-identifying* if the sets  $K_r(v)$  are all nonempty and different, that is, every pair of vertices are *r-separated* and each vertex is *r-covered* by at least one codeword.

Although the aim of this paper is to construct identifying codes over  $\mathcal{G}(M)$  graphs, the problem over the infinite mesh will be considered before. Previous

papers dealing with the problem of identification over the infinite mesh are, for example, [7], [10] and [6]. Therefore, let us define the infinite mesh as the Cayley graph  $\text{Cay}(\mathbb{Z}^2, E)$ . This graph will be denoted as  $\mathbb{Z}^2$  whenever there is no possibility of confusion. Also, the elements in  $\mathbb{Z}^2$  will be in column form, for convenience. The following new definitions will be also needed.

**Definition 3.2.** The following subsets of  $\mathbb{Z}^2$  are defined:

$$\begin{aligned}\mathcal{UR}_r^- &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid 0 \leq x, y \wedge |x| + |y| = r \right\} \\ \mathcal{UL}_r^- &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x \leq 0 \leq y \wedge |x| + |y| = r \right\} \\ \mathcal{BR}_r^- &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid y \leq 0 \leq x \wedge |x| + |y| = r \right\} \\ \mathcal{BL}_r^- &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x, y \leq 0 \wedge |x| + |y| = r \right\} \\ \mathcal{UR}_r^+ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid 0 < x, y \wedge |x| + |y| = r + 1 \right\} \\ \mathcal{UL}_r^+ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x < 0 < y \wedge |x| + |y| = r + 1 \right\} \\ \mathcal{BR}_r^+ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid y < 0 < x \wedge |x| + |y| = r + 1 \right\} \\ \mathcal{BL}_r^+ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x, y < 0 \wedge |x| + |y| = r + 1 \right\}\end{aligned}$$

The translated sets are denoted as  $\mathcal{UR}_r^-(v) = v + \mathcal{UR}_r^-$  and analogously for the other sets. A graphical representation of these sets is shown in Figure 2.

The next definition and lemma will be useful to prove the identifiability of the codes proposed in this paper.

**Definition 3.3.** Let  $\mathcal{C}$  be a code of a graph  $\mathcal{G}(M)$  and  $v$  be a vertex. The ball  $B_r(v)$  is said to be  $r$ -fixed by  $\mathcal{C}$  if there exists at least a codeword in each one of the next sets:

$$\mathcal{UR}_r^-(v) \cup \mathcal{BL}_r^+(v), \mathcal{UL}_r^-(v) \cup \mathcal{BR}_r^+(v), \mathcal{BR}_r^-(v) \cup \mathcal{UL}_r^+(v), \mathcal{BL}_r^-(v) \cup \mathcal{UR}_r^+(v)$$

**Remark 1.** Although having the ball in every vertex  $r$ -fixed is not a sufficient condition to be  $r$ -identifying (as the example in Figure 3), this property will be used as a first step in the proofs, since it simplifies them.

**Lemma 3.4.** If  $G$  is a Cayley graph over a group  $\Gamma$  and  $\mathcal{C}$  is a subgroup of  $\Gamma$ , then  $\mathcal{C}$  is a code such that for all  $c \in \mathcal{C}$ ,  $K_r(v + c) = c + K_r(v)$ .

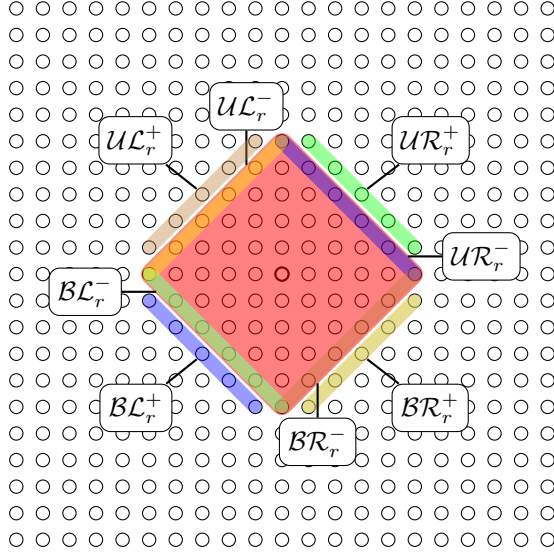


Figure 2: Subsets that divide the periphery of the  $r$ -ball.

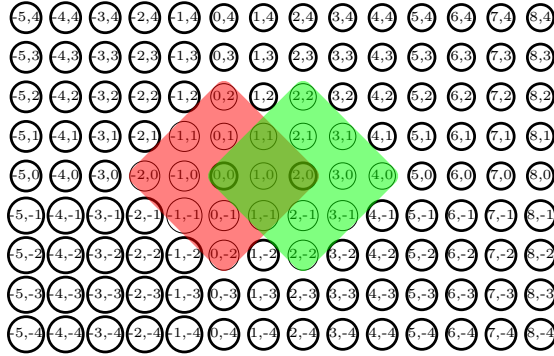


Figure 3: Every ball is 2-fixed, but it is not 2-identifying.

## 4 The Construction of Identifying Codes

In this section a wide family of identifying codes over the infinite mesh will be constructed. Then, by making the suitable modular operation by a matrix  $M$ , these codes will also be identifying over a graph  $\mathcal{G}(M)$ .

Let  $t$  and  $d$  be two positive integers. Let us consider the code

$$\mathcal{C} = \left\langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \right\rangle$$

of the infinite mesh. Also,  $C = \begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix}$  will denote the matrix associated to the group code. If  $N$  denotes the cardinal of  $\mathbb{Z}^2/\mathcal{C}\mathbb{Z}^2$ , it is obtained that  $N = \det(C) = t^2 + (t+d)^2$ . Note that, as it was proved in [15], the covering radius of the code  $\mathcal{C}$  is  $t+d$ .

In the next subsections it will be determined the radius  $r$  such that  $\mathcal{C}$  is  $r$ -identifying over  $\mathbb{Z}^2$ . Depending on  $t$  and  $d$  there are three cases:

1. if  $\gcd(2t, d) = 1$  then  $\mathcal{C}$  is  $r$ -identifying for  $r = t^2 + dt + (d^2 - 1)/2$ ,
2. if  $\gcd(2t, d) = 2$  then  $\mathcal{C}$  is  $r$ -identifying for  $r = t^2 + dt + d^2/2$ ,
3. if  $\gcd(2t, d) \geq 3$  then  $\mathcal{C}$  is not  $r$ -identifying for any  $r$ .

As a consequence, the covering radius is quite smaller than the identifying. This will be beneficial for the identification process as it will be remarked in Section 5. Moreover, sufficient conditions for  $\mathcal{C}$  to be also  $r$ -identifying over  $\mathcal{G}(M)$  will be given. Finally, the density of the construction will be considered.

### 4.1 First Case: $\gcd(2t, d) = 1$

Let  $t$  and  $d$  be two positive integers such that  $\gcd(2t, d) = 1$ . Let us consider the code  $\mathcal{C} = \left\langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \right\rangle$  over  $\mathbb{Z}^2$  and let us denote by  $N$  the volume of the fundamental parallelogram of  $\mathcal{C}$ , that is,  $N = \det(C) = t^2 + (t+d)^2$ . The following technical result can be proved:

**Lemma 4.1.** *If  $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{C}$  then for every  $m, n \in \mathbb{Z}$ ,  $\begin{pmatrix} x + mN \\ y + nN \end{pmatrix} \in \mathcal{C}$ .*

*Proof.* The result is obtained by

$$\begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix} \begin{pmatrix} t+d \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ N \end{pmatrix},$$

and

$$\begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix} \begin{pmatrix} t \\ -t-d \end{pmatrix} = \begin{pmatrix} N \\ 0 \end{pmatrix}.$$

□

**Lemma 4.2.** For all  $v \in \mathbb{Z}^2$ ,  $B_r(v)$  is  $r$ -fixed by  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \rangle$ , where  $r = t^2 + dt + \frac{d^2-1}{2}$  and  $\gcd(2t, d) = 1$ .

*Proof.* It will be proved that for each  $v \in \mathbb{Z}^2$  there exists a codeword  $c$  in the set  $\mathcal{UR}_r^-(v) \cup \mathcal{BL}_r^+(v)$ . The other three codewords can be obtained by making the suitable rotations. Note that, if  $c \in \mathcal{UR}_r^-(v) \cup \mathcal{BL}_r^+(v)$  and  $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  then  $Rc$  is codeword in  $\mathcal{UL}_r^-(Rv) \cup \mathcal{BR}_r^+(Rv)$ ,  $R^2c$  is codeword in  $\mathcal{BL}_r^-(R^2v) \cup \mathcal{UR}_r^+(R^2v)$  and  $R^3c$  is codeword in  $\mathcal{BR}_r^-(R^3v) \cup \mathcal{UL}_r^+(R^3v)$ .

Since  $c$  must be in  $\mathcal{C}$ , there must exist  $a, b \in \mathbb{Z}$  such that  $c = \begin{pmatrix} at - b(t+d) \\ a(t+d) + bt \end{pmatrix}$ .

Now, if  $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ , let us denote  $\begin{pmatrix} x \\ y \end{pmatrix} = c - v$ . Then, the following system of Diophantine equations is obtained:

$$\begin{cases} x = at - b(t+d) - v_1 \\ y = a(t+d) + bt - v_2 \end{cases}$$

Therefore,  $x + y = a(2t + d) - bd - v_1 - v_2$ . By hypothesis,  $\gcd(2t + d, d) = \gcd(2t, d) = 1$ , which implies that there exist  $a_0, b_0 \in \mathbb{Z}$  such that  $a_0(2t + d) - b_0d = r + v_1 + v_2$ . Thus, there also exist  $x_0, y_0 \in \mathbb{Z}$  such that  $x_0 + y_0 = r$ . The set of solutions is  $\{a' = a_0 + d\lambda, b' = b_0 + (2t + d)\lambda \mid \lambda \in \mathbb{Z}\}$ . Therefore, let  $x' = a_0t - b_0(t+d) + td\lambda - (t+d)(2t+d)\lambda - v_1 = a_0t - b_0(t+d) - v_1 - N\lambda = x_0 - \lambda N$  and in the same way let  $y' = y_0 + \lambda N$ .

Now, it is set  $\lambda$  such that  $0 \leq x' < N = 2r + 1$ , so  $0 \leq x' \leq 2r$ . Two different cases are obtained:

- If  $0 \leq x' \leq r$  then it is obtained that  $0 \leq y' \leq r$ . Therefore, taking  $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$  implies that  $c = v + \begin{pmatrix} x \\ y \end{pmatrix}$  is in  $\mathcal{UR}_r^-(v)$ .
- Otherwise, it is obtained that  $r < x' \leq 2r$  so  $-r \leq y' < 0$ . Therefore, taking  $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' - N \\ y' \end{pmatrix}$  (which is a codeword by Lemma 4.1) implies that  $x + y = r - N = -r - 1$  and  $-r - 1 < x \leq -1$ , that is  $-r \leq x < 0$ , thus obtaining that  $c = v + \begin{pmatrix} x \\ y \end{pmatrix}$  is a codeword in  $\mathcal{BL}_r^+(v)$ .

□

**Theorem 4.3.** Let  $t, d$  be positive integers such that  $\gcd(2t, d) = 1$  and  $r = t^2 + dt + \frac{d^2-1}{2}$ . Then,  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \rangle$  is a  $r$ -identifying code in  $\mathbb{Z}^2$ .

*Proof.* By the previous lemma, all  $r$ -balls are  $r$ -fixed, and hence,  $\mathcal{C}$   $r$ -dominates  $\mathbb{Z}^2$ . However, this is not enough for being an  $r$ -identifying code. Therefore, it will be next proved that any  $v \in \mathbb{Z}^2$  is  $r$ -separated from  $w = v + \begin{pmatrix} x \\ y \end{pmatrix}$ , for any



$\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$ . Note that, if  $|x| = |y|$  this is straightforward since the balls are  $r$ -fixed. Then, as each 90-degree rotation leaves  $\mathcal{C}$  invariant, it can be assumed without loss of generality that  $x > y \geq 0$ .

If there is a codeword in  $\mathcal{UL}_r^-(v)$  then it is straightforward that they are  $r$ -separated. Otherwise, there is a codeword  $c_1 \in \mathcal{C} \cap \mathcal{BR}_r^+(v)$  which is not in  $K_r(v)$ . If  $c_1$  is in  $K_r(w)$  the proof has finished. As  $c_1 \in \mathcal{BR}_r^+(v)$  it can be expressed as  $c_1 = v + \begin{pmatrix} a \\ a - r - 1 \end{pmatrix}$  with  $1 \leq a \leq r$ . Then,

$$c_1 + \begin{pmatrix} -(t+d) \\ t \end{pmatrix} = v + \begin{pmatrix} a - (t+d) \\ a + t - r - 1 \end{pmatrix}$$

is a codeword which is further from  $K_r(w)$  than  $c_1$ . And when  $a > \frac{d-1}{2}$ , it is in  $K_r(v)$ .

If the same than in the previous case is done, but for  $\mathcal{BL}_r^-(v) \cup \mathcal{UR}_r^+(v)$ , it is obtained that  $c_2 = v + \begin{pmatrix} b \\ r - b + 1 \end{pmatrix} \in \mathcal{UR}_r^+(v)$ . Then,

$$c_2 + \begin{pmatrix} -(t+d) \\ t \end{pmatrix} - \begin{pmatrix} t \\ t+d \end{pmatrix} = c_2 + \begin{pmatrix} -2t-d \\ -d \end{pmatrix} = v + \begin{pmatrix} b - 2t - d \\ r - b - d + 1 \end{pmatrix}$$

which is further from  $K_r(w)$  than  $c_2$  and when  $b > t$  it is in  $K_r(v)$ .

To finish, it has to be proved that the case when both codewords  $c_1, c_2$  are in the left ranges never happens. For that, let us assume that  $1 \leq a \leq \frac{d-1}{2}$  and  $1 \leq b \leq t$ , with  $c_1, c_2 \in \mathcal{C}$ . Thus,  $c = c_1 - c_2 = \begin{pmatrix} a - b \\ a + b - 1 - N \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$  is in the rectangle defined by:

$$\{1 - t \leq x' < \frac{d-1}{2} - 1 < d, 1 - N \leq y' \leq t + \frac{d-1}{2} - 1 - N < t + d - N\}$$

which does not include the point  $\begin{pmatrix} 0 \\ -N \end{pmatrix}$ . This rectangle is a subset of

$$\{1 - 2t \leq x' \leq -t, -N \leq y' \leq -N + t - 1\} \cup \{1 - t \leq x' \leq d, -N \leq y' \leq -N + t + d - 1\}$$

which is a set of representatives of  $\mathbb{Z}^2/\mathcal{C}\mathbb{Z}^2$  (see [11]) and contains  $\begin{pmatrix} 0 \\ -N \end{pmatrix}$ . As a consequence, all its elements are different. Therefore,  $c$  is not congruent with  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  and thus it is not a codeword, which is a contradiction.  $\square$

Once a family of identifying codes over  $\mathbb{Z}^2$  has been constructed, new conditions have to be added in order to get an identifying code also over  $\mathcal{G}(M)$ . The

most obvious condition is that the code must be periodic. Then, in the case of these lattice codes  $M$  has to be a multiple of the matrix  $C$  associated to the lattice code. With this it is obtained that the code is locally the same than in the plane, thus keeping its density. The second condition is that any ball cannot overlap with itself. These conditions are stated in the following result.

**Corollary 1.** *Let  $t, d$  be two positive integers and  $M \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$ . Let us consider the graph  $\mathcal{G}(M)$  and its code  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \rangle$ . If there exists  $Q \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$  such that  $M = CQ$  and  $\min\{d(0, M\gamma) \mid 0 \neq \gamma \in \mathbb{Z}^2\} > 2r + 1$  then  $\mathcal{C}$  is a  $r$ -identifying code in  $\mathcal{G}(M)$  for  $r = t^2 + dt + \frac{d^2-1}{2}$ .*

**Remark 2.** Note that  $\min\{d(0, M\gamma) \mid 0 \neq \gamma \in \mathbb{Z}^2\}$  is the length of the shortest non-trivial cycle in  $\mathcal{G}(M)$ .

In [16] it was shown that, under some conditions for matrix  $M$ ,  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+1 \end{pmatrix}, \begin{pmatrix} -t-1 \\ t \end{pmatrix} \rangle$  is a perfect  $t$ -error correcting code over the graph  $\mathcal{G}(M)$ . Moreover, this is the only perfect code that can be constructed over that graph, up to symmetries. Next, this result about perfect codes and the previous one obtained in this section dealing with identifying codes are summarized in the following corollary.

**Corollary 2.** *Let  $t$  be a positive integer and  $M \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$ . Let us consider the graph  $\mathcal{G}(M)$  and its code  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+1 \end{pmatrix}, \begin{pmatrix} -(t+1) \\ t \end{pmatrix} \rangle$ . If there exists  $Q \in \mathcal{M}_{2 \times 2}(\mathbb{Z})$  such that  $M = CQ$  and  $\min\{d(0, M\gamma) \mid 0 \neq \gamma \in \mathbb{Z}^2\} > 2t(t+1) + 1$  then  $\mathcal{C}$  is a  $t(t+1)$ -identifying and  $t$ -perfect code in  $\mathcal{G}(M)$ .*

**Example 4.4.** Let us consider  $t = 1$  and the matrix  $M = \begin{pmatrix} 25 & 0 \\ 0 & 25 \end{pmatrix}$ . Then, the code  $\mathcal{C} = \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix} \rangle$  is 2-identifying in  $\mathcal{G}(M)$  which, as it can be seen in Figure 4, is a square torus graph of side 25.

**Example 4.5.** Let us consider the Kronecker graph product of cycles of lengths 20 and 5. In [21], it was shown that the code  $\mathcal{C} = \langle \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \end{pmatrix} \rangle$  is a 1-perfect code over this graph. It can be seen that this graph is  $\mathcal{G}(M; A)$ , with matrix  $M = \begin{pmatrix} 20 & 0 \\ 0 & 5 \end{pmatrix}$  and set of adjacencies  $A = \{ \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \}$ . As it was proved in [16], this graph is isomorphic to  $\mathcal{G}(M')$ , where  $M' = \begin{pmatrix} 10 & -5 \\ 10 & 5 \end{pmatrix}$ . Now, using the previous method it is obtained that the code  $\mathcal{C} = \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix} \rangle$  is 1-perfect, but also 2-identifying in  $\mathcal{G}(M)$ . Note that the codes are the same by the graph isomorphism, but our method allows us to determine also the identifying radius

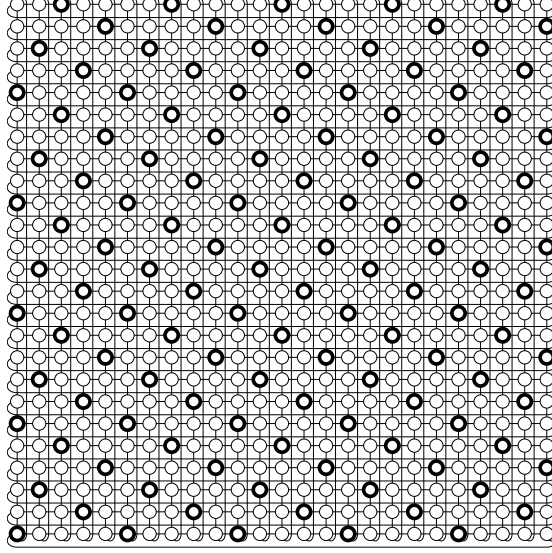


Figure 4: 1-Perfect and 2-identifying over the torus graph.

of the code. In Figure 5, the Kronecker product and the code are represented. In Figure 6 its isomorphic Cayley graph and the transformed code are shown.

#### 4.2 Second Case: $\gcd(2t, d) = 2$

Let  $t$  and  $d$  be two positive integers such that  $\gcd(2t, d) = 2$ . Again, let us consider the code  $\mathcal{C} = \left\langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \right\rangle$  over  $\mathbb{Z}^2$  and let us denote by  $N = \det\left(\begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix}\right) = 2t^2 + 2td + d^2$  the volume of its fundamental parallelogram. It can be proved that:

**Lemma 4.6.**  $\begin{pmatrix} N/2 \\ N/2 \end{pmatrix}$  and  $\begin{pmatrix} N/2 \\ -N/2 \end{pmatrix}$  are codewords in  $\mathcal{C}$ .

*Proof.* The proof is just to check that the following equalities hold:

$$\begin{pmatrix} N/2 \\ N/2 \end{pmatrix} = \begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix} \begin{pmatrix} t+d/2 \\ -d/2 \end{pmatrix},$$

$$\begin{pmatrix} N/2 \\ -N/2 \end{pmatrix} = \begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix} \begin{pmatrix} -d/2 \\ t+d/2 \end{pmatrix}.$$

□

**Lemma 4.7.** For all  $v \in \mathbb{Z}^2$ ,  $B_r(v)$  is  $r$ -fixed by  $\mathcal{C}$ , where  $r = t^2 + dt + \frac{d^2}{2}$  and  $\gcd(2t, d) = 2$ .

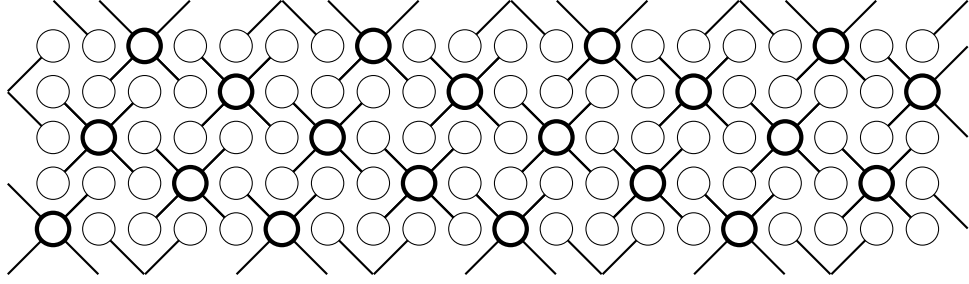


Figure 5: 1-perfect code over Kronecker product of cycles.

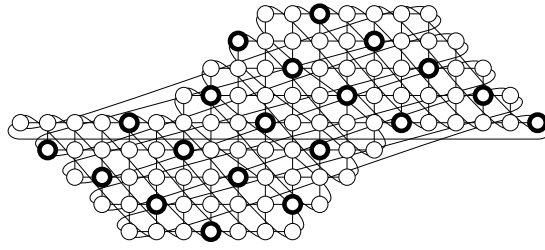


Figure 6: 2-identifying and 1-perfect code over  $\mathcal{G}(M)$ .

*Proof.* Analogously to the proof of Lemma 4.2 the following system of Diophantine equations is obtained:

$$\begin{cases} x = at - b(t + d) - v_1 \\ y = a(t + d) + bt - v_2 \end{cases}$$

Therefore,  $x + y = a(2t + d) - bd - v_1 - v_2$ . By hypothesis,  $\gcd(2t + d, d) = \gcd(2t, d) = 2$ , which implies that there exist  $a_0, b_0 \in \mathbb{Z}$  such that  $a_0(2t + d) - b_0d = r + v_1 + v_2$  or  $a_0(2t + d) - b_0d = r + 1 + v_1 + v_2$ . Thus, there also exist  $x_0, y_0 \in \mathbb{Z}$  such that  $x_0 + y_0 = r$  or  $x_0 + y_0 = r + 1$ . The set of solutions is  $\{a' = a_0 + \frac{d}{2}\lambda, b' = b_0 + (t + \frac{d}{2})\lambda \mid \lambda \in \mathbb{Z}\}$ . Therefore, let  $x' = a_0t - b_0(t + d) + t\frac{d}{2}\lambda - (t + \frac{d}{2})(t + d)\lambda - v_1 = x_0 - \lambda\frac{N}{2}$  and in the same way let  $y' = y_0 + \lambda\frac{N}{2}$ .

Now, let us set  $\lambda$  such that  $0 < x' \leq \frac{N}{2} = r$ . Hence,  $y' < x' + y' \leq r + y'$ . If  $x' + y' = r$  then  $0 \leq y' < r$  and  $c$  is at  $\mathcal{UR}_r^-(v)$ , otherwise  $x' + y' = r + 1$  with  $0 < y' < r + 1$  and  $c$  is at  $\mathcal{UR}_r^+(v)$ .  $\square$

**Remark 3.** Note that it has been proved something stronger than being  $r$ -fixed, that is, every ball has a codeword in each of the four sets  $\mathcal{UL}_r^-, \mathcal{UR}_r^-, \mathcal{BL}_r^-, \mathcal{BR}_r^-$  or in each of the four sets  $\mathcal{UL}_r^+, \mathcal{UR}_r^+, \mathcal{BL}_r^+, \mathcal{BR}_r^+$ .

**Theorem 4.8.** *Let  $t, d$  be positive integers such that  $\gcd(2t, d) = 2$ . Then,  $\mathcal{C} = \langle \binom{t}{t+d}, \binom{-(t+d)}{t} \rangle$  is an  $r$ -identifying code in  $\mathbb{Z}^2$  for  $r = t^2 + dt + \frac{d^2}{2}$ .*

*Proof.* By previous Lemma 4.7, all  $r$ -balls are  $r$ -fixed. Now, it has to be proved that any  $v \in \mathbb{Z}^2$  is  $r$ -separated from  $w = v + \binom{x}{y}$ , for any  $\binom{x}{y} \in \mathbb{Z}^2$ . First, as in the proof of Theorem 4.3 it can be assumed that  $x > y \geq 0$ . As a consequence of Remark 3 it can be assumed that there are codewords in each of  $\mathcal{UL}_r^+(v), \mathcal{UR}_r^+(v), \mathcal{BL}_r^+(v), \mathcal{BR}_r^+(v)$ . Let  $c_1 \in \mathcal{C} \cap \mathcal{BR}_r^+(v)$  which is not in  $K_r(v)$ . If  $c_1$  is in  $K_r(w)$  the proof is finished.

Since  $c_1 \in \mathcal{BR}_r^+(v)$ , this implies that it can be expressed as  $c_1 = v + \binom{a}{a-r-1}$ . Then,

$$c_1 + \binom{-(t+d)}{t} = v + \binom{a-(t+d)}{a+t-r-1}$$

is a codeword which is further from  $K_r(w)$  than  $c_1$ . When  $a > \frac{d}{2}$ , it is in  $K_r(v)$ .

Proceeding analogously, but for  $\mathcal{UR}_r^+(v)$ , it is obtained that  $c_2 = v + \binom{b}{r-b+1}$ . Then, let us consider

$$c_2 + \binom{-(t+d)}{t} - \binom{t}{t+d} = c_2 + \binom{-2t-d}{-d} = v + \binom{b-2t-d}{r-b-d+1}$$

which is further from  $K_r(w)$  than  $c_2$  and when  $b > t$  it is in  $K_r(v)$ .

Finally, the case when both codewords  $c_1, c_2$  are in the left ranges has to be analyzed. For that, when  $1 \leq a \leq \frac{d}{2}$  and  $1 \leq b \leq t$ , with  $c_1, c_2 \in \mathcal{C}$  is obtained that  $c = c_1 - c_2 \in \mathcal{C}$ . Then,  $c = c_1 - c_2 = \begin{pmatrix} a - b \\ a + b - 1 - N \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$  is in the rectangle defined by:

$$\{1 - t \leq x' \leq \frac{d}{2} - 1 < d, -N \leq y' \leq t + \frac{d}{2} - N - 2 < t + d - N\}$$

which includes the point  $\begin{pmatrix} 0 \\ -N \end{pmatrix}$ . This rectangle is a subset of the set of representatives of  $\mathbb{Z}^2 / \mathcal{C}\mathbb{Z}^2$

$$\{1 - 2t \leq x' \leq -t, -N \leq y' \leq -N + t - 1\} \cup \{1 - t \leq x' \leq d, -N \leq y' \leq -N + t + d - 1\}$$

and consequently, all its elements are different. Therefore,  $c$  is the only element congruent with  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  (using Lemma 4.6) and thus  $x' = 0$  and  $y' = -N$ . Follows that  $a = b = 1$  and  $c_1 = \begin{pmatrix} 1 \\ -r \end{pmatrix}$ . If  $x = 1$  then  $c_1$  separates  $v$  from  $w$ . If  $x > 1$  then  $c_1 + \begin{pmatrix} -\frac{N}{2} \\ \frac{N^2}{2} \end{pmatrix} = \begin{pmatrix} 1 - r \\ 0 \end{pmatrix}$  (which is another codeword by Lemma 4.6) separates  $v$  from  $w$ .  $\square$

**Remark 4.** Note that, if  $N = \det(C)$  denotes the volume of the fundamental parallelogram of the lattice code  $\mathcal{C}$ , in both cases  $r = \lfloor \frac{N}{2} \rfloor$  is the identifying radius. In the first case, that is  $\gcd(2t, d) = 1$ , by computational analysis it has been observed that the obtained radius in Theorem 4.3 seems to be the minimal one. However, in this second case, smaller radii have been found that make the code also identifying. For example, it has been observed that in many cases  $t^2 + (d - 1)t + \frac{d^2 - d + 1}{2}$  is also a possible radius of identification, which is smaller than the one given in Theorem 4.8.

### 4.3 Third Case: $\gcd(2t, d) \geq 3$

In previous subsections it has been computed the radius  $r$  such that the code  $\mathcal{C} = \langle \begin{pmatrix} t \\ t + d \end{pmatrix}, \begin{pmatrix} -(t + d) \\ t \end{pmatrix} \rangle$  is  $r$ -identifying over the lattice  $\mathbb{Z}^2$ , wherever  $t$  and  $d$  are two positive integers such that  $\gcd(2t, d) \leq 2$ . In this subsection it is established that, in any other election for  $t$  and  $d$ , the lattice code  $\mathcal{C}$  is not  $r$ -identifying, for any  $r \in \mathbb{Z}$ .

**Lemma 4.9.** *For any group code  $\mathcal{C}$  over  $\mathbb{Z}^2$  for which there exists  $\begin{pmatrix} x \\ y \end{pmatrix}$  such*

that there is no codeword in any of the subsets:

$$\begin{aligned}\ell_1 &= \left\{ \begin{pmatrix} x+k \\ y+k \end{pmatrix} \mid k \in \mathbb{Z} \right\}, \\ \ell_2 &= \left\{ \begin{pmatrix} x+k \\ y-k \end{pmatrix} \mid k \in \mathbb{Z} \right\}, \\ \ell_3 &= \left\{ \begin{pmatrix} x+k \\ y+k+1 \end{pmatrix} \mid k \in \mathbb{Z} \right\} \text{ and} \\ \ell_4 &= \left\{ \begin{pmatrix} x+k \\ y-k+1 \end{pmatrix} \mid k \in \mathbb{Z} \right\},\end{aligned}$$

then,  $\mathcal{C}$  is not an identifying code for any radius.

*Proof.* The proof is made by *reductio ad absurdum*. Therefore, let us assume that  $\mathcal{C}$  identifies for the radius  $r \in \mathbb{N}$ . Let  $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$  be the vertex of the hypothesis. The translations of  $\ell_i$  are referred as diagonals and two diagonals  $\ell_a, \ell_b$  are contiguous when  $\ell_a = \ell_b \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . For example,  $\ell_1$  and  $\ell_3$  are two contiguous diagonals. First note that for any two contiguous diagonals, at least one must be codewordless. Otherwise, since  $\mathcal{C}$  is a group, there would be codewords in all diagonals. Moreover, if there is a codeword in a diagonal  $\ell$ , then the two contiguous diagonals in both directions  $(\ell + \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ell + \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \ell - \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ell - \begin{pmatrix} 0 \\ 2 \end{pmatrix})$  must be codewordless.

Now, consider the word  $w = \begin{pmatrix} x \\ y-r-1 \end{pmatrix}$ . The following diagonals at the bottom of the ball  $B_r(w)$  are denoted by:

$$\begin{aligned}\ell'_1 &= \left\{ \begin{pmatrix} x+k \\ y+k-2r-2 \end{pmatrix} \mid k \in \mathbb{Z} \right\} & \ell'_2 &= \left\{ \begin{pmatrix} x+k \\ y-k-2r-2 \end{pmatrix} \mid k \in \mathbb{Z} \right\} \\ \ell'_3 &= \left\{ \begin{pmatrix} x+k \\ y+k-2r-1 \end{pmatrix} \mid k \in \mathbb{Z} \right\} & \ell'_4 &= \left\{ \begin{pmatrix} x+k \\ y-k-2r-1 \end{pmatrix} \mid k \in \mathbb{Z} \right\} \\ \ell'_5 &= \left\{ \begin{pmatrix} x+k \\ y+k-2r \end{pmatrix} \mid k \in \mathbb{Z} \right\} & \ell'_6 &= \left\{ \begin{pmatrix} x+k \\ y-k-2r \end{pmatrix} \mid k \in \mathbb{Z} \right\}\end{aligned}$$

Note that  $w$  is at distance  $r+1$  from  $v$ , and hence from  $\ell_1$  and  $\ell_2$ . Also,  $v$  is at distance  $r+2$  from  $\ell_3$  and  $\ell_4$ . Since  $\ell'_1$  and  $\ell'_2$  are at distance  $r+1$  from  $w$ , it will be said that they are *outer* of  $B_r(w)$ . Also, since  $\ell'_3, \ell'_4$  at distance  $r$  it will be said that they are *inner* of  $B_r(w)$ . At least one of  $\ell'_1, \ell'_3$  is codewordless and the same happens for  $\ell'_2, \ell'_4$ . In Figure 7 an example of the relative locations of  $v, w$  and the diagonals is shown. Now, three different cases are considered according to the location of the codewords with respect to the diagonals, that is  $\ell'_1, \ell'_2$  outside and  $\ell'_3, \ell'_4$  inside:

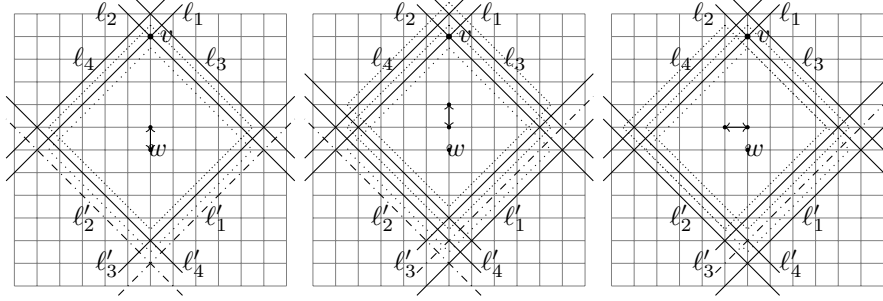


Figure 7: Possibilities for the diagonals

1. All the diagonals with codewords (0, 1 or 2) are outer diagonals. In the figure  $\ell'_1$  and  $\ell'_2$  are dashed, indicating that they have some codeword, all other diagonals are solid, indicating that they have no codewords. As diagonals  $\ell'_3$  and  $\ell'_4$  are codewordless it is obtained that  $K_r(w) \subseteq K_r(w + \begin{pmatrix} 0 \\ 1 \end{pmatrix})$ . Since the same is true for  $\ell_3$  and  $\ell_4$ , it is obtained that  $K_r(w + \begin{pmatrix} 0 \\ 1 \end{pmatrix}) \subseteq K_r(w)$ . Thus  $K_r(w) = K_r(w + \begin{pmatrix} 0 \\ 1 \end{pmatrix})$  and they are not separable. In the figure it can be seen that in the symmetric difference of the two balls there are only solid lines, which indicates the non separability.
2. Two diagonals with codewords are inner, or 1 is inner and 1 is outer. Since two contiguous diagonals above any diagonal with a codeword must be codewordless and one of  $\ell'_1, \ell'_3$  has a codeword, then  $\ell'_5$  is codewordless. Respectively, since  $\ell'_2$  or  $\ell'_4$  has a codeword then  $\ell'_6$  is codewordless. Now, we have the same position as in the previous item of the proof, but translated by  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  and that  $K_r(w + \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = K_r(w + \begin{pmatrix} 0 \\ 2 \end{pmatrix})$ . Hence, they are not separable.
3. Only one diagonal with codewords is inner. Without loss of generality let us assume that  $\ell'_3$  is the inner diagonal with some codeword. Therefore, it is obtained that  $\ell'_1, \ell'_2, \ell'_4$  and  $\ell'_5$  are codewordless. Analogously to the previous cases, but for  $w + \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  and  $w + \begin{pmatrix} -1 \\ 1 \end{pmatrix}$  implies that  $K_r(w + \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = K_r(w + \begin{pmatrix} -1 \\ 1 \end{pmatrix})$  are not separable.

In all cases non-separable codewords have been found, which contradicts the  $r$ -identifiability of  $\mathcal{C}$  and thus the proof is completed.  $\square$

**Theorem 4.10.** *Let  $t, d$  be two positive integers such that  $\gcd(2t, d) \geq 3$ . Then, the code  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+d \end{pmatrix}, \begin{pmatrix} -(t+d) \\ t \end{pmatrix} \rangle$  is not identifying for any radius over  $\mathbb{Z}^2$ .*



*Proof.* A codeword  $\begin{pmatrix} x \\ y \end{pmatrix}$  of  $\mathcal{C}$  satisfies that there exist  $a, b \in \mathbb{Z}$  such that:

$$\begin{cases} x = at - b(t + d) \\ y = a(t + d) + bt \end{cases}$$

Let  $h$  be an integer such that  $y = x + h$ , so  $h = ad + b(2t + d)$  is obtained. Hence,  $\gcd(2t + d, d) = \gcd(2t, d)$  divides  $h$ . This implies that the contiguous diagonals  $\left\{ \begin{pmatrix} k \\ k + h \end{pmatrix} \mid k \in \mathbb{Z} \right\}$  are codewordless for  $0 < h < \gcd(2t, d)$ .

When  $\gcd(2t, d) \geq 3$ , at least two contiguous diagonals have not codeword. Since the code is invariant under rotations, contiguous orthogonal diagonals are also codewordless. Thus  $\mathcal{C}$  satisfies the hypothesis of the Lemma 4.9 and therefore, it is not identifying for any radius.  $\square$

#### 4.4 On the Density of the Construction

Several papers have been developed for the computation of identifying codes attaining the minimal density bounds. To define the density of a code over  $\mathbb{Z}^2$ , let us denote by  $Q_n$  the set of vertices  $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$  with  $|x| \leq n$  and  $|y| \leq n$ . Then, the *density* of a code  $\mathcal{C}$  is defined as:

$$D(\mathcal{C}) = \lim_{n \rightarrow \infty} \sup \frac{|\mathcal{C} \cap Q_n|}{|Q_n|}.$$

In [7] there is a compilation of lower and upper bounds of the best possible density for codes in some infinite regular graphs, in terms of the identifying radius. For the case of the square grid it is obtained that:

$$\frac{3}{8r + 4} \leq D(r) \leq \begin{cases} \frac{2}{5r} & \text{if } r \text{ even,} \\ \frac{2r}{5r^2 - 2r + 1} & \text{if } r \text{ odd.} \end{cases}$$

In particular, in [3] it was proved for 1-identifying codes that:

**Theorem 4.11.** [3] *The minimum density of 1-identifying codes in  $\mathbb{Z}^2$  is  $\frac{7}{20}$ .*

In the following, the density for our construction of identifying codes is calculated. Although the values are not far from the optimal one, they are established here since they can be exactly computed in order to complete our study.

**Lemma 4.12.** *Let  $\mathcal{G}(M)$  be such that  $\mathcal{C} = \left\langle \begin{pmatrix} t \\ t + d \end{pmatrix}, \begin{pmatrix} -(t + d) \\ t \end{pmatrix} \right\rangle$  is an  $r$ -identifying code. Then, the density of  $\mathcal{C}$  is*

$$D(r) = \begin{cases} \frac{1}{2r+1} & \text{if } r \text{ is odd,} \\ \frac{1}{2r} & \text{if } r \text{ is even.} \end{cases}$$

*Proof.* Let  $C = \begin{pmatrix} t & -(t+d) \\ t+d & t \end{pmatrix}$ . By definition of density,:

$$D(r) = \lim_{n \rightarrow \infty} \frac{|\mathcal{C} \cap Q_n|}{|Q_n|} = \frac{|\mathcal{C}|}{|V|} = \frac{\frac{\det(M)}{\det(C)}}{\det(M)} = \frac{1}{\det(C)}.$$

Now, since  $\det(C) = t^2 + (t+d)^2 = 2r+1$  or  $2r$ , the result is straightforwardly obtained.  $\square$

**Remark 5.** The corresponding code in  $\mathbb{Z}^2$  has the same density.

Although the constructed codes have a little higher density than the best constructions they form a wide family and its regularity may have practical applications. This fact will be highlighted in next section, where it is taken advantage of the inclusion of perfect codes in our family of identifying codes.

## 5 Adaptive Identification in Cayley Graphs

In this section the implications of the constructed codes in adaptive identification is considered. Firstly, the approach for adaptive identification presented in [2] and [20] is summarized. Then, our proposal for identifying faults with the codes presented in this paper is stated. Finally, a detailed example of this proposal is addressed.

In [2, 20], *adaptive identification* is defined as a game. In that game, a player secretly chooses a vertex (or none) of the graph and another player tries to find it by making successive queries. For any vertex  $v$  of the graph, the queries are of the type:

“Is the chosen vertex in  $B_r(v)$ ?”

and these queries are answered truthfully.

If  $\mathcal{C}$  is a  $r$ -identifying code, then the chosen vertex can be found by making queries only to vertices in  $\mathcal{C}$ . As proposed in [2], the identification can be done in two stages, in order to minimize the number of performed queries. The first stage consist on making queries in a  $r$ -covering code that is intended to be near perfect. Thus, this  $r$ -covering is used to find out the ball  $B_r(c)$  which contains the chosen vertex. In the second stage, using the  $r$ -identifying code, the vertex is determined. That is, two different codes with the same parameter  $r$  being the covering and identification radii, respectively, are used to identify the selected vertex. As a consequence, at least three kind of vertices coexist in the graph: vertices belonging to the  $r$ -covering, vertices belonging to the  $r$ -identifying and the rest of the vertices of the graph.

The proposal in the present paper is to use the same code for both stages, instead of having two different codes. As it was proved in Corollary 2,  $t$ -perfect codes of the form  $\mathcal{C} = \langle \begin{pmatrix} t \\ t+1 \end{pmatrix}, \begin{pmatrix} -(t+1) \\ t \end{pmatrix} \rangle$  are also  $r$ -identifying codes for  $r = t(t+1)$ . Moreover, although they are not the most dense as identifying codes, they are not very far from the bound. Thus, in this alternative configuration

there will be only two kind of vertices: codewords and non-codewords. On the contrary, there will be two kind of queries (for different radius  $t$  and  $r$ ), both for any codeword  $c \in \mathcal{C}$ . The first query is of the type:

“Is the chosen vertex in  $B_t(c)$ ?”

and the second one of the type:

“Is the chosen vertex in  $B_r(c)$ ?”

Therefore, in the first stage of the method the perfect code will be used to determine if there is a faulty vertex. If so, the vertex that detects the faulty vertex initiates the identification process.

Identifying codes have been motivated several times as a good strategy to locate faulty nodes in a multiprocessor system, although they have not been applied at the moment. In such a system, the existence of a faulty node is the exceptional case. Hence, it is important that the first stage of the identification, which is just the detection of the fault, is optimized. This is the reason why in our proposal the detection of the faulty node and consequently its bound inside a ball or radius  $r$  is made with a perfect code. Then, since the second stage (to locate the faulty vertex exactly) would be the exceptional situation, the requirements on the identification radius have been relaxed.

Finally, to illustrate this method, an example of this application is detailed next. Let us consider the graph  $\mathcal{G}(M)$  defined by  $M = \begin{pmatrix} 28 & -4 \\ 4 & 28 \end{pmatrix}$ , which is graphically represented in Figure 8. Let us also consider the code defined by the group  $\mathcal{C} = \langle \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} -4 \\ 3 \end{pmatrix} \rangle$  which is also represented in the figure. By Corollary 2, this is a 3-perfect code and a 12-identifying code over  $\mathcal{G}(M)$ . Note that the graph has  $\det(M) = 800$  vertices and the code has  $\frac{800}{25} = 32$  codewords. Then, following the adaptive strategy detailed above, for each codeword  $c \in \mathcal{C}$  it is periodically checked if there is a faulty vertex in  $B_3(c)$  by performing queries of the first type. Then, if and only if the obtained answer is positive, the second stage of the identification is started by the same codeword.

Assume that for example node  $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$  has failed, which is represented in bold. Then, the first stage of the procedure detects a faulty vertex and bound it in a ball of 25 vertices, whose center is in this case the codeword  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ , as can be observed in Figure 9. Then, that codeword starts the identification stage by making queries in  $B_{12}(c)$  balls, as shown in Figure 10. Therefore, with a binary decision tree of depth  $\lceil \log_2(25) \rceil = 5$  as the one in Figure 11, the faulty node can be isolated. Each vertex of the tree represents the realization of a query of the second type, continuing by the branch which matches the answer. Branches to the left represent positive answers to the question “Is the faulty vertex in  $B_{12}(c)$ ”. On the contrary, branches to the right represent negative answers. In this particular case, node  $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$  is identified by the path of queries:

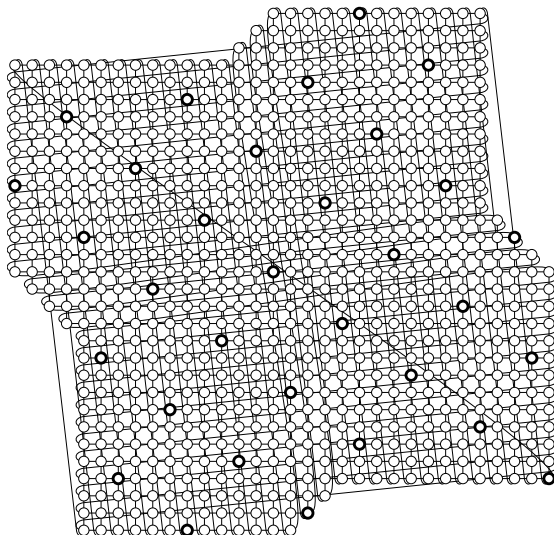


Figure 8: A 3-perfect and 12-identifying code.

$$\begin{pmatrix} 2 \\ 11 \end{pmatrix} \rightarrow \begin{pmatrix} -11 \\ 2 \end{pmatrix} \rightarrow \begin{pmatrix} 8 \\ -6 \end{pmatrix} \rightarrow \begin{pmatrix} 6 \\ 8 \end{pmatrix} \rightarrow \begin{pmatrix} 10 \\ 5 \end{pmatrix}.$$

In non-adaptive identification all the codewords are checked, that is  $|\mathcal{C}| = 32$  queries of radius  $r$  are done. Our proposal makes 32 queries of radius  $t = 3$  and then, when necessary, 5 queries of radius  $r = 12$ .

## 6 Conclusions

In this paper a method for constructing a wide family of identifying codes over Cayley graphs of degree four defined by means of Abelian groups has been presented. These graphs include many previously known topologies for interconnection networks such as tori, twisted tori [18], Midimews [1] and double loops in general [9]. The codes are constructed by means of subgroups of the generating group of the Cayley graph. As a consequence, the codewords are regularly distributed over the lattice so that the covering radius is relatively small. The identifying radius is characterized in terms of the generators of the subgroup as well as the covering radius. Moreover, some of the codes not only are identifying but also perfect. Therefore, the diagnosis process can be separated into two stages: a first stage for detecting the existence of a failure (using the small covering radius) and the identification of the corresponding vertex (using the identifying radius). Taking advantage of these facts, the adaptive identification process has been considered and a practical example of how it would perform has been addressed in the present paper. This special feature of

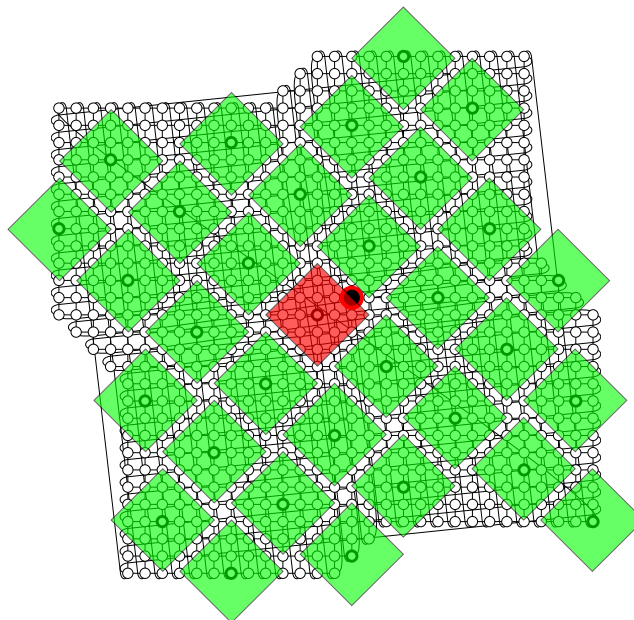


Figure 9: Querying  $B_t(c)$  for each codeword, locating a faulty vertex.

the codes which are obtained with our method would make possible to assert that the construction gives suitable codes for a practical scenario.

## Acknowledgments

This work has been supported by the Spanish Ministry of Science under contracts TIN2010-21291-C02-02, AP2010-4900 and CONSOLIDER Project CSD2007-00050, and by the European HiPEAC Network of Excellence.

## References

- [1] R. Beivide, E. Herrada, J. L. Balcázar, and A. Arruabarrena. Optimal distance networks of low degree for parallel computers. *IEEE Trans. Comput.*, 40(10):1109–1124, 1991.
- [2] Y. Ben-Haim, S. Gravier, A. Lobstein, and J. Moncel. Adaptive identification in graphs. *J. Comb. Theory Ser. A*, 115:1114–1126, October 2008.
- [3] Y. Ben-Haim and S. Litsyn. Exact minimum density of codes identifying vertices in the square grid. *SIAM J. Discret. Math.*, 19:69–82, May 2005.

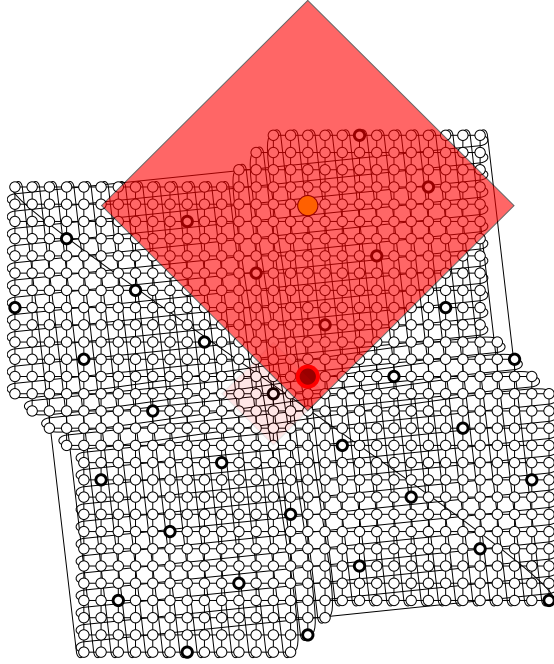


Figure 10: Querying a ball  $B_r(c)$  centered in a codeword.

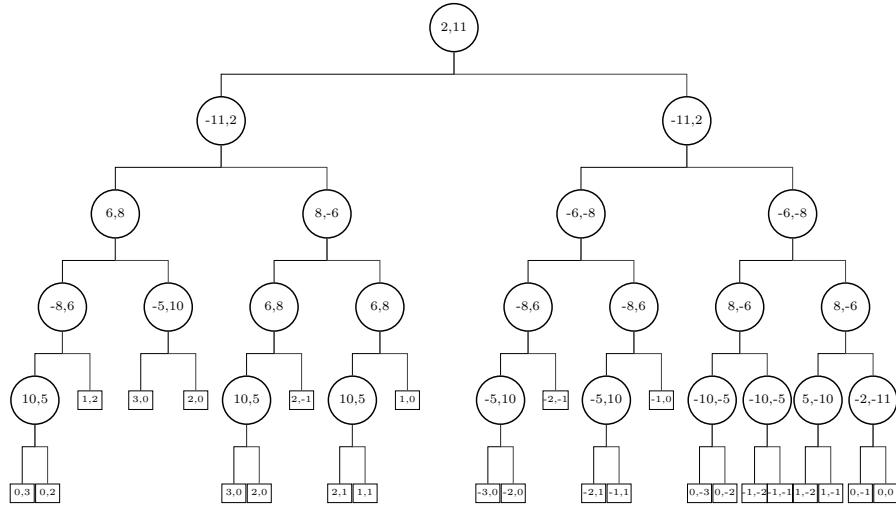


Figure 11: Binary decision tree for identification.

- [4] J.-C. Bermond, O. Favaron, and M. Maheo. Hamiltonian decomposition of Cayley graphs of degree 4. *Journal of Combinatorial Theory, Series B*, 46(2):142 – 153, 1989.
- [5] C. Camarero, C. Martínez, and R. Beivide. Identifying codes over L-graphs. In *Accepted for presentation at the 3th International Castle Meeting on Coding Theory and Applications (3ICMTA)*, 2011.
- [6] I. Charon, I. Honkala, O. Hudry, and A. Lobstein. General bounds for identifying codes in some infinite regular graphs. *The Electronic Journal of Combinatorics*, 2001.
- [7] I. Charon, O. Hudry, and A. Lobstein. Identifying codes with small radius in some infinite regular graphs. *The Electronic Journal of Combinatorics*, 2002.
- [8] M. Fiol. On congruence in  $\mathbb{Z}^n$  and the dimension of a multidimensional circulant. *Discrete Math*, 141:1–3, 1995.
- [9] M. Fiol, J. L. A. Yebra, I. Alegre, and M. Valero. Discrete optimization problem in local networks and data alignment. *IEEE Trans. Comput.*, 36(6):702–713, 1987.
- [10] I. Honkala and A. Lobstein. On the density of identifying codes in the square lattice. *J. Comb. Theory Ser. B*, 85:297–306, June 2002.
- [11] J. H. Jordan and C. J. Potratz. Complete residue systems in the Gaussian integers. *Mathematics Magazine*, 38(1):pp. 1–12, 1965.
- [12] M. Karpovsky, K. Chakrabarty, and L. Levitin. On a new class of codes for identifying vertices in graphs. *Information Theory, IEEE Transactions on*, 44(2):599–611, Mar. 1998.
- [13] A. Lobstein. Watching systems, identifying, locating-dominating and discriminating codes in graphs. <http://www.infres.enst.fr/~lobstein/debutBIBidetlocdom.pdf>.
- [14] M. Malek. A comparison connection assignment for diagnosis of multiprocessor systems. In *Proceedings of the 7th annual symposium on Computer Architecture*, ISCA '80, pages 31–36, New York, NY, USA, 1980. ACM.
- [15] C. Martinez, R. Beivide, E. Stafford, M. Moreto, and E. M. Gabidulin. Modeling toroidal networks with the Gaussian integers. *IEEE Transactions on Computers*, 57:1046–1056, 2008.
- [16] C. Martínez, C. Camarero, and R. Beivide. Perfect graph codes over two dimensional lattices. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1047–1051, june 2010.

- [17] F. P. Preparata, G. Metze, and R. T. Chien. On the connection assignment problem of diagnosable systems. *Electronic Computers, IEEE Transactions on*, EC-16(6):848–854, dec. 1967.
- [18] C. H. Sequin. Doubly twisted torus networks for VLSI processor arrays. In *ISCA '81: Proceedings of the 8th annual symposium on Computer Architecture*, pages 471–480, Los Alamitos, CA, USA, 1981. IEEE Computer Society Press.
- [19] C. K. Wong and D. Coppersmith. A combinatorial problem related to multimodule memory organizations. *J. ACM*, 21(3):392–402, 1974.
- [20] A. L. Y. Ben-Haim, S. Gravier and J. Moncel. Adaptive identification in torii in the king lattice. *Electronic Journal of Combinatorics*, 18:116, May 2011.
- [21] J. Zernovnik. Perfect codes in direct products of cycles—a complete characterization. *Advances in Applied Mathematics*, 41(2):197–205, 2008.